Pubblica Amministrazione, Biblioteche e Trasformazione digitale: uno sguardo d'insieme

Valdo Pasqui

Il 2017 è stato un anno ricco di novità per l'evoluzione verso il digitale della Pubblica Amministrazione sia sul piano normativo che su quello strategico e dopo la fase di gestazione fin troppo lunga del Piano Triennale 2017-2019 per l'informatica nella Pubblica Amministrazione il percorso per l'attuazione concreta sembra avviato sebbene con la ormai consueta lentezza che contraddistingue l'innovazione nel nostro paese. Siamo di fronte ad un quadro molto articolato e complesso che implica un significativo impegno di risorse umane, intellettuali, organizzative e tecnologiche e che richiede una costante attenzione anche a causa dei ritardi con i quali il Legislatore ha ottemperato agli i adempimenti di sua competenza, in parte ancora da completare, dando luogo a frammentazioni, sovrapposizioni e lasciando anche alcuni vuoti.

Lo sforzo al quale sono chiamati tutti gli operatori coinvolti nei processi delle Pubbliche Amministrazioni non riguarda soltanto l'adozione di alcune tecnologie innovative e di nuovi servizi ma comporta un significativo sforzo per razionalizzare i servizi e infrastrutture e per sostituire il principio di responsabilità in materia di sicurezza e trattamento dei dati personali al posto del pedissequo adempimento delle norme tramite l'adozione di regole minimali. Siamo dunque di fronte ad un cambiamento di mentalità che richiede consapevolezza, formazione, informazione e la condivisione efficacie di processi nei quali comunque il fattore umano mantiene un ruolo determinante nonostante la presenza sempre più invasiva delle tecnologie informatiche e telematiche (ICT). Le biblioteche hanno anticipato da anni questa trasformazione adeguando e facendo evolvere i loro servizi, elaborando piani di sviluppo e attivando percorsi per aggiornamento continuo delle competenze dei bibliotecari. L'articolo cerca di fornire un quadro di riferimento sintetico e integrato delle norme, dei provvedimenti, dei piani e delle strategie in atto ed esamina cinque temi di rilevate interesse al fine di fornire una traccia di lettura che consenta alle biblioteche di orientarsi in questo complesso contesto.

Breve viaggio dei più recenti provvedimenti

Gran parte dei provvedimenti riguardano il recepimento di normative e regolamenti europei che hanno richiesto l'adeguamento delle norme già vigenti e devono essere ancora completati dall'approvazioni di decreti attuativi.

Il Decreto Legislativo 7 marzo 2005, n. 82, conosciuto come Codice per l'Amministrazione Digitale (CAD), dopo vari interventi di modifica, integrazione e abrogazione di articoli e commi intervenuti negli anni (tra i quali una sostanziale modifica con il Dlgs. 26 agosto 2016, n. 179) è approdato alla sua ultima versione, la sesta, con la pubblicazione nella Gazzetta Ufficiale del 12 gennaio 2018 del Dlgs 13 dicembre 2017 n. 217[1]. Tale decreto recepisce quanto previsto dal Regolamento (UE) 23

[1] https://cad.readthedocs.io/it/v2017-12-13/

luglio 2014, n. 910, noto come "Regolamento eIDAS", che regolamenta l'identificazione elettronica e servizi fiduciari per le transazioni elettroniche (documento informatico, identificazione, firme elettroniche, PEC e servizi di conservazione digitale) con lo scopo di «rafforzare la fiducia nelle transazioni elettroniche nel mercato interno fornendo una base comune per interazioni elettroniche sicure fra cittadini, imprese e autorità pubbliche». Inoltre il nuovo CAD estende le prerogative dell'AgiD istituendovi la figura del Difensore civico digitale (Art.17), definisce il domicilio digitale (Art.3 bis), stabilisce che non sarà più necessario conservare la copia dei documenti informatici scambiati con la Pubblica amministrazione poiché se ne faranno carico le stesse amministrazioni alle quali in qualunque momento sarà possibile richiederne l'accesso (Art.43), istituisce la "Piattaforma digitale nazionale dati" (Art. 50 ter) realizzata dall'ISTAT per valorizzare il patrimonio informativo detenuto dalle amministrazioni, rafforza il principio del riuso del sw stabilendo che «le pubbliche amministrazioni che siano titolari di soluzioni e programmi informatici realizzati su specifiche indicazioni del committente pubblico, hanno l'obbligo di rendere disponibile il relativo codice sorgente» (Art. 69). Infine, sostituisce (Art. 1) le regole tecniche previste in precedenza con «Linee guida contenenti le regole tecniche e di indirizzo» adottate dall'AgID previa consultazione pubblica. A proposito di questo ultimo articolo, essenziale per poter rendere operativa in pratica gran parte del CAD, è bene precisare che per ora, in mancanza di queste linee guida, continuano a valere le precedenti regole tecniche[2].

Nell'ambito del trattamento dei dati personali il Regolamento (UE) 2016/679 del Parlamento Europeo (L 119/34), noto come General Data Protection Regulation (GDPR), approvato il 27 aprile 2016 e pubblicato nella GU UE il 4 maggio del 2016, dà tempo agli Stati Membri fino al 24 maggio 2018 per l'aggiornamento della propria legislazione. In Italia solo lo scorso 21 marzo 2018 il Comunicato stampa n.75 del Consiglio dei Ministri ha annunciato l'approvazione dello Schema di Decreto Legislativo che introduce disposizioni per l'adeguamento della normativa nazionale alle disposizioni del GDPR (in attuazione dell'Art. 13 della Legge di delegazione europea 2016-2017, legge 25 ottobre 2017, n. 163). Questo Dlgs, ancora non pubblicato, prevede l'abrogazione del Codice in materia di protezione dei dati personali (Dlgs 30 giugno 2003, n. 196) dal prossimo 25 maggio. E' facile immaginare la complessità amministrativa per l'adeguamento a cominciare dalla necessità di modificare tutta la modulistica esistente facente riferimento al Dlgs 196/2003, al rifacimento di tutte le informative sul trattamento dati, mentre la maggior parte della Amministrazioni e delle aziende private sono in ritardo per adeguamenti ai nuovi principi del GDPR.

Vi è poi il contesto della trasformazione digitale del nostro Paese il cui indirizzo strategico ed economico è stato formulato attraverso il "Piano Triennale per l'Informatica nella Pubblica Amministrazione 2017-2019" il quale definisce un modello di riferimento per lo sviluppo

[2] Le regole tecniche vigenti sono:
- DPCM 22 febbraio 2013 (Regole tecniche in materia di firme elettroniche)
- DPCM 3 dicembre 2013 (Regole tecniche in materia di protocollo informatico)
- DPCM 3 dicembre 2013 (Regole tecniche in materia di conservazione)
- DMEF 17 giugno 2014 (regole tecniche in materia di conservazione dei documenti
- fiscalmente rilevanti),
- DPCM 13 novembre 2014 (regole tecniche sui documenti informatici).

dell'informatica pubblica italiana. Dopo la presentazione dell'Agenda Digitale da parte della Commissione Europea nel maggio 2010, sottoscritta da tutti gli Stati membri, il 1° marzo 2012 è stata istituita l'Agenda Digitale Italiana che conteneva le premesse per la creazione e lo sviluppo di un ecosistema della Pubblica Amministrazione digitale. Ma si è dovuto attendere l'ottobre e il novembre del 2014 per la pubblicazione rispettivamente della strategia per la Banda Ultra Larga e della strategia per la Crescita Digitale elaborate dalla Presidenza del Consiglio dei Ministri insieme al Ministero dello Sviluppo Economico, all'Agenzia per l'Italia Digitale (AgID) e all'Agenzia per la Coesione per il perseguimento degli obiettivi dell'Agenda Digitale Europea in Italia. Dopo una fase di consultazione pubblica il 3 marzo 2015 il Consiglio dei ministri ha approvato il «Piano nazionale Banda Ultra Larga» e il piano per la «Crescita Digitale 2014-2020»[3]. All'AgID è stato attribuito il compito di garantire la realizzazione di questi obiettivi in coerenza con l'Agenda digitale europea. Il CAD, nell'articolo Art. 14-bis definisce le funzioni dell'Agenzia per l'Italia Digitale (AgID) stabilendo nel primo comma che AgID «è preposta alla realizzazione degli obiettivi dell'Agenda Digitale Italiana, in coerenza con gli indirizzi dettati dal Presidente del Consiglio dei ministri o dal Ministro delegato, e con l'Agenda digitale europea».

Tuttavia gli sviluppi e gli eventi più consistenti e concreti si sono verificati proprio nei mesi più recenti. Finalmente il 1 giugno 2017 il Consiglio dei Ministri ha approvato il «Piano Triennale 2017-2019 per l'informatica nella Pubblica Amministrazione»[4]. Questo lungo percorso si è infine concluso nel mese di febbraio 2018 con la firma dell'Accordo Quadro, di durata triennale, per la Crescita e la Cittadinanza Digitale Verso Gli Obiettivi Europa 2020 tra AgID, Regioni e Province Autonome[5]. In sintesi il piano:

a) formula l'indirizzo strategico ed economico attraverso la definizione di un modello di riferimento per lo sviluppo dell'informatica pubblica italiana;
b) definisce la strategia operativa di trasformazione digitale dell'Italia;
c) traccia il percorso per conseguire l'obiettivo di risparmio della spesa annuale per la gestione corrente del settore informatico della PA;
d) riconosce alle Regioni, attraverso l'Accordo Quadro, il ruolo di coordinamento a livello territoriale nel favorire la trasformazione digitale dei servizi pubblici per i cittadini e imprese.

Il Piano si articola nelle seguenti aree d'intervento:

- Infrastrutture fisiche (*data center*, c*loud* e connettività)
- Infrastrutture immateriali (dati della PA, piattaforme abilitanti)
- Interoperabilità
- Ecosistemi
- Strumenti per la generazione e la diffusione di servizi digitali
- Sicurezza

[3] http://www.agid.gov.it/notizie/2015/03/24/approvati-i-piani-nazionali-la-banda-ultralarga-crescita-digitale

[4] https://pianotriennale-ict.italia.it/

[5] http://trasparenza.agid.gov.it/archivio28_provvedimenti_0_121528_791_1.html

- Data & Analytics Framework
- Gestione del cambiamento e monitoraggio

Per concludere questo rapido *excursus* occorre ricordare come sia diventato di pressante attualità il tema della sicurezza telematica (*cybersecurity*) che coinvolge in modo trasversale tutti gli ambiti precedenti. La Direttiva del Parlamento europeo 2016/1148 «recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione» in vigore dal 19 luglio 2016 definisce un quadro generale al fine di armonizzare i comportamenti e le azioni degli Stati membri «in materia di sicurezza della rete e dei sistemi informativi a livello nazionale» e di attivare livelli di integrazione sul piano organizzativo per aumentare la capacità di protezione, reazione e intervento nel caso di attacchi ed eventi che rechino pregiudizio alla disponibilità, autenticità, integrità e riservatezza dei «dati conservati o trasmessi o trattati e dei relativi servizi offerti o accessibili tramite tale rete o sistemi informativi».

I documenti digitali al centro

Il *Regolamento UE 910/2014 del 23 luglio 2014 identificazione elettronica e servizi fiduciari per le transazioni elettroniche* (eIDAS) afferma il principio che una transazione elettronica non può essere respinta per il solo motivo di essere in forma elettronica e si prefigge l'obiettivo di assicurare che a un documento elettronico non dovrebbero essere negati gli effetti giuridici a causa della sua forma elettronica. Partendo da queste premesse l'Art. 3 definisce come *documento elettronico* «qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva».

Il CAD nella sia formulazione originaria (Dlgs n. 82 7 marzo 2005) definiva il «documento informatico» come «la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti», ma già con le modifiche del Dlgs 26 agosto 2016, n. 179 si è adeguato al Regolamento europeo rimpiazzando la precedente con la seguente definizione: «il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti» (Art.1) e rinviando per la definizione di documento elettronico in modo esplicito al Regolamento eIDAS (Art.1 comma 1-bis). E' opportuno sottolineare che questa definizione di documento elettronico comprende due aspetti complementari e fortemente integrati: i) "qualsiasi contenuto"; ii) "conservato in forma elettronica". Con il primo elemento si fornisce piena dignità e rilevanza ad ogni contenuto digitale indipendentemente dalla sua tipologia (testo, registrazione sonora, visiva o audiovisiva), con il secondo si include e sottolinea che il processo di conservazione è indispensabile. Da questa premessa discende il rafforzamento nel CAD dei principi attinenti la formazione dei documenti informatici (Art.40), la validità ed efficacia probatoria dei documenti informatici (Art.20), le precisazioni riguardo i documenti amministrativi informatici (l'Art.23-ter comma 1 riporta: «Gli atti formati dalle pubbliche amministrazioni con strumenti informatici, nonché i dati e i documenti informatici detenuti dalle stesse, costituiscono informazione primaria ed originale») e quelle relativi al procedimento e al fascicolo informatico (Art. 41). Più controverso invece quanto previsto in materia di conservazione dei documenti dall'Art. 43 comma 1-bis che elimina l'obbligo di conservazione da parte dei cittadini e delle imprese quando il documento informatico è conservato per legge dalle PA, imponendo alle stesse amministrazioni l'obbligo di renderli accessibili online attraverso gli strumenti di identificazione previsti dal Sistema pubblico per la gestione delle identità digitali (SPID) (Art.64). La natura controversa del suddetto comma dell'Art.43 risiede primariamente nella lentezza con la quale

le PA si stanno adeguando a questo processo di trasformazione al digitale in particolare per quanto riguarda la conservazione a norma, spesso non applicata neppure ai documenti previsti in base a specifiche normative (es. le fatture elettroniche), la gestione dei procedimenti e dei fascicoli elettronici e l'adozione di SPID.

I ritardi accumulati non sono imputabili soltanto alla carenza di personale o alla limitazione di risorse economiche per l'integrazione e l'aggiornamento dei servizi, ma dipendono anche dalla lentezza delle PA e del loro personale, molto spesso fin dai livelli apicali, nel ripensare, riprogettare e riorganizzare i processi interni affinché i procedimenti amministrativi siano svolti avvalendosi degli strumenti informatici. Siamo in presenza di un *gap* culturale che non consente di sfruttare al meglio le potenzialità offerte dalle tecnologie ICT r indice a conservare processi e modalità organizzative senza attivare efficaci strategie di razionalizzazione e continuando a produrre, manipolare e scambiare grandi quantità di documenti cartacei, con inutile aggravio di costi sia dal punto di vista economico che ecologico, di tempi e di impegno. L'inerzia, e la resistenza, nel processo di trasformazione verso il digitale sono state ampiamente messe in evidenza dalla Relazione della Commissione Parlamentare d'Inchiesta sulla Digitalizzazione e l'Innovazione della PA[6], Comunicata alla Presidenza della Camera dei deputati il 26 ottobre 2017, che rivela come la maggioranza delle pubbliche amministrazioni non abbia provveduto alla nomina del responsabile alla transizione digitale (Art. 17 del CAD). La Relazione sottolinea che le PA si affidano «ancora troppo alla carta, disattendendo la legge che impone di formare gli originali dei propri documenti con mezzi informatici sin dalla prima versione dell'articolo 40 del CAD, mentre la dematerializzazione degli atti è ancora a livelli insufficienti ed insoddisfacenti» e rileva carenze nelle competenze digitali, un numero insufficiente di ore dedicate alla formazione in ICT e l'assenza nei piani delle performance di indicatori riferiti alla trasformazione digitale e di obiettivi bene definiti relativi alle azioni da intraprendere. Nelle conclusioni, riassumendo le criticità emerse, la Relazione asserisce che «Le pubbliche amministrazioni, nella grande maggioranza dei casi, approcciano il tema del digitale in modo episodico e non organico. Sicuramente non strategico e non prioritario».

A questo proposito sembra opportuno rilevare che biblioteche in Italia hanno svolto un ruolo pionieristico prima con lo sviluppo di servizi per l'accesso alle risorse digitali (riviste elettroniche, banche dati bibliografiche e specialistiche), poi con la costituzione di repository digitali e attraverso la realizzazione di applicazioni per la condivisione ed il prestito di materiale audiovisivo e multimediale. Per prime le biblioteche si sono poste il problema della conservazione digitale a lungo termine (*digital preservation*) delle risorse digitali che ormai costituiscono una parte sempre più rilevante del loro patrimonio e dei servizi a disposizione dei loro utenti. Le competenze maturate negli ultimi veni anni dai bibliotecari nella metadatazione, classificazione, organizzazione, fruizione e conservazione delle risorse digitali e nello sviluppo di servizi integrati e usabili per garantire l'accessibilità alle risorse costituiscono un patrimonio di riferimento di innegabile rilevanza di cui tutte le PA potrebbero avvalersi per recuperare i ritardi accumulati affrontando percorsi formativi e progetti innovativi.

6

http://www.camera.it/_dati/leg17/lavori/documentiparlamentari/IndiceETesti/022bis/014/INTERO.pdf

Servizi “abilitanti” e Basi di dati di interesse nazionale

Nel processo di trasformazione al digitale della PA in Italia occorre ricordare anche il ruolo svolto dalle biblioteche pubbliche con lo sviluppo dei cataloghi in linea (OPAC) fin dagli anni ottanta e la loro rapida evoluzione grazie al web, la diffusione degli strumenti di ricerca delle banche dati bibliografici, lo sviluppo dell’ecosistema digitale del Servizio Bibliotecario Nazionale incentrato sull’Indice SBN e il prestito ILL SBN, il catalogo nazionale dei periodici (ACNP). Per questo stride a fronte di questo impegno e dei relativi risultati l’assenza nel Piano triennale di qualunque riferimento a SBN e ai sistemi bibliotecari.

La mappa di dettaglio del Modello strategico di evoluzione del sistema informativo della PA del Piano triennale per l’informatica nella pubblica amministrazione contempla un insieme di *ecosistemi verticali* tra i quali quello comprendente i beni culturali e il turismo. Le *infrastrutture immateriali* hanno lo scopo di standardizzare, razionalizzare i e semplificare lo sviluppo dei servizi digitali delle PA e comprendono le basi di dati di interesse nazionale, gli open data, e i vocabolari controllati (*Dati della PA*) e i servizi infrastrutturali condivisi tra le PA (*Piattaforme abilitanti*). Il CAD (Art.60 comma 3-bis) individua le seguenti basi di dati di interesse nazionale:

- repertorio nazionale dei dati territoriali
- anagrafe nazionale della popolazione residente (ANPR)
- banca dati nazionale dei contratti pubblici
- casellario giudiziale;
- registro delle imprese;
- gli archivi automatizzati in materia di immigrazione e di asilo (e Art.2, comma 2, DPR 27 luglio 2004, n. 242)
- Anagrafe nazionale degli assistiti (ANA)
- anagrafe delle aziende agricole (ex Art. 1, comma 1, del regolamento di cui l DPR 1 dicembre 1999, n. 503)

A queste il Piano triennale aggiunge altre banche dati quali:

- l’Indice delle Pubbliche amministrazioni (IPA)
- l’Indice nazionale degli indirizzi di posta elettronica certificata di professionisti e imprese
- il Catalogo dei dati delle Pubbliche amministrazioni
- l’Anagrafe tributaria e la Base dati catastale dell’Agenzia delle Entrate
- l Pubblico registro automobilistico (PRA) dell’ACI.

Le sezioni del Piano dedicate a queste componenti e i report sullo stato di avanzamento dei servizi già operativi o in fase di sviluppo non contengono riferimenti all’ambito delle biblioteche, tra le banche dati strategiche non sono citate SBN, ACNP e l’Anagrafe delle biblioteche. Tra i servizi abilitanti figurano i poli di conservazione documentale, in larga parte ancora da realizzare salvo realtà come ParER in Emilia Romagna, che tuttavia riguardano la conservazione dei documenti dei procedimenti amministrativi. Non vi è invece traccia di obiettivi e strategie relativi alla creazione di servizi per la conservazione nel lungo periodo di risorse digitali (*digital preservation*) né per il deposito legale. Il Progetto Magazzini Digitali dovrebbe assumere un ruolo prioritario proprio per la conservazione a lungo termine delle risorse elettroniche delle biblioteche e vi è la necessità di

sviluppare una rete di servizi destinati a questo scopo al fine della conservazione dei contenuti digitali che ormai sono parte integrante e sempre più rilevante del patrimonio culturale da preservare per le future generazioni. AIB si è attivata per dialogare con AgID al fine di integrare e valorizzare il patrimonio di basi di dati e sevizi esistente tra quelli previsti nel Piano.

Se può lasciare perplessi che nel Piano la cultura sia quasi esclusivamente vista in funzione della valorizzazione turistica dell'Italia, un altro aspetto quantomeno singolare è rappresentato dal fatto che nel portale *dati.gov.it I dati aperti della Pubblica Amministrazione* la categoria "cultura" è aggregata con "istruzione" e sport". In tale raggruppamento la ricerca con la parola "biblioteche" fornisce come risultato 53 dataset, la ricerca per "archivi" o "archivio" ne rende in tutto 84 in maggioranza di carattere demografico, quella per "musei" restituisce 42 risultati e quella per "fotografico" solo 8.

Per quanto riguarda le piattaforme abilitanti il Piano triennale comprende:

- CIE (Carta d'identità elettronica):
- SPID (Sistema pubblico d'identità digitale)
- PagoPa (Gestione elettronica dei pagamenti verso la PA)
- Fatturazione elettronica
- ComproPA: sistema nazionale di e-procurement (in fase di sviluppo)
- Sistema di avvisi e notifiche di cortesia (in fase di sviluppo)
- SIOPE+, evoluzione del sistema SIOPE, per l'analisi e la valutazione della spesa, il monitoraggio e il controllo dei conti pubblici (in fase di sviluppo)
- NoiPA: evoluzione dell'attuale sistema di gestione del personale (in fase di sviluppo)
- Sistema di gestione dei procedimenti amministrativi nazionali: garantisce la comunicazione digitale tra cittadini e PA attraverso lo strumento del domicilio digitale (in fase di sviluppo)
- Poli di conservazione per l'erogazione di servizi di conservazione documentale (in fase di sviluppo)

Il sito AgID "Avanzamento trasformazione digitale"[7] al 12 aprile 2018 riporta 87 milioni di fatture elettroniche, 13.018 PA attive in PagoPA con oltre 7.300.000 pagamenti, 108 comuni subentrati in ANPR per oltre 1.900.000 abitanti, oltre 2.300.000 identità SPID erogate e 4.000 amministrazioni attive, poco più di 20.100 dataset open data per sole 385 amministrazioni. Sia PagoPA che SPID per il momento hanno avuto un'adesione molto inferiore a quanto atteso e il numero di servizi della PA integrati con questi due strumenti è ancora limitato seppur in continua crescita.

L'ecosistema dei servizi delle biblioteche può trarre notevole beneficio dall'adozione di SPID e di PagoPA. L'adesione delle biblioteche a PagoPA offre il vantaggio di ridurre la complessità ammnistrativa, tecnica e gestionale per l'attivazione di servizi di pagamento online (es. tramite POS virtuali) e consente al fruitore di utilizzare diverse modalità di pagamento attraverso una piattaforma trasversale per tutti i servizi di pagamento verso le PA. L'implementazione di SPID nei portali dei sistemi bibliotecari può indubbiamente facilitare la registrazione e l'accesso da parte degli utenti, operazione che con tale integrazione può avvenire interamente online e consentendo al cittadino dotato di SPID di accreditarsi e accedere ai servizi di più biblioteche con le stesse credenziali e senza

[7] https://avanzamentodigitale.italia.it/it

recarsi presso la biblioteca. Naturalmente questo approccio non deve essere visto come uno stravolgimento del rapporto diretto tra cittadino-utente e biblioteca-istituzione, la presenza fisica negli spazi della biblioteca e il contatto con i bibliotecari restano un fattore integrante dei servizi e della stessa missione delle biblioteche, tuttavia la semplificazione e la sburocratizzazione possono facilitare l'avvicinamento da parte di soggetti sempre più abituati ad operare in rete. Nel portale SPID di AgiD attraverso il motore di ricerca che permette di individuare i servizi abilitati con SPID le uniche biblioteche presenti sono il Servizio Bibliotecario del Comune di Reggio Emilia e quelli aderenti alla ReteINDACO del Comune di Roma. Tuttavia nel secondo caso dopo essersi registrati con successo tramite SPID al Portale del Comune di Roma nel momento in cui si naviga e si esce verso il portale dei servizi Biblioteche di Roma (BiblioTu) scegliendo l'edicola o uno degli altri servizi video e audiolibri quando si prova ad accedere alla risorsa non si viene riconosciuti e il pannello di autenticazione o registrazione non prevede la modalità SPID. Molti Atenei che hanno implementato l'accesso ai propri servizi online tramite SPID hanno integrato anche l'accesso ai servizi bibliotecari.

Dismissione dei data center e l'evoluzione verso il Cloud

Il CAD affida all'AgiD (Art. 14-bis comma 2) i compiti di predisporre il Piano triennale per l'informatica nella pubblica amministrazione, di verificarne la successiva attuazione e di monitorare le attività svolte dalle pubbliche amministrazioni inclusi gli investimenti effettuati e la loro coerenza con il Piano Triennale. Quest'ultimo nel Capitolo 12 richiama in modo esplicito la Circolare AgID n. 2 del 24 giugno 2016 sulle "Modalità di acquisizione di beni e servizi ICT…" affermando che «le Pubbliche amministrazioni non possono costituire nuovi data center». Dunque quale è il futuro dei cosiddetti "centri elaborazione dati" e come si prefigura il nuovo scenario delle infrastrutture preposte all'erogazione dei servizi delle PA?

Le linee d'azione del Piano triennale (par. 3.1.3) definiscono un modello nel quale questi centri sono destinati rapidamente a scomparire e ad essere rimpiazzati dai Poli strategici nazionali (PSN). I PSN devono rispettare "i requisiti di capacità, eccellenza tecnica, economica ed organizzativa" che AgID ha individuato con la Circolare 5 del 30 novembre 2017 stabilendo anche una specifica procedura di qualificazione. I PSN potranno anche svolgere funzioni di conservazione dei documenti.

Attraverso un censimento svolto da AgiD tutte le PA attualmente dotate di infrastrutture fisiche saranno suddivise in due gruppi A e B. Nel primo rientrano quelle i cui data center non sono stati eletti come PSN o con carenze strutturali o organizzative considerate minori, nel secondo quelle i cui centri «non garantiscono requisiti minimi di affidabilità e sicurezza dal punto di vista infrastrutturale e/o organizzativo, o non garantiscono la continuità dei servizi». La differenza tra le due categorie consiste nel fatto che le PA appartenenti alla prima, pur senza poter effettuare investimenti per l'ampliamento o l'evoluzione, potranno continuare ad operare con la propria infrastruttura fino al completamento della migrazione o verso i servizi messi a disposizione da CONSIP attraverso il Contratto quadro SPC-Cloud lotto 1 o verso un PSN, invece quelle rientranti nella seconda devono migrare «rapidamente» ad una delle due precedenti soluzioni.

E' evidente che a causa della rapida obsolescenza delle infrastruttura e della continua necessità di adeguare le capacità dei data center questo insieme di prescrizioni impedisce il consueto processo evolutivo, che di solito si volge secondo cicli della durata di 3-5 anni, e obbliga le PA ad anticipare

processi di dismissione per acquisire i servizi della gara SPC-Cloud o consolidare i propri servizi su data center costituiti con altre PA, a livello regionale, in attesa di qualificarsi come PSN.

Il Piano triennale ha previsto una *road-map* per intraprendere e portare a compimento questo processo i cui passaggi prevedevano entro febbraio 2018 l'avvio dell'adeguamento dei data center delle PA scelte come Poli strategici nazionali e il consolidamento dei servizi delle PA del gruppo B su un PSN o sul SPC-Cloud Lotto 1. A seguire, da aprile 2018, le PA devono aver predisposto i propri piani di razionalizzazione ed essere pronte a fornirlo ad Agid in caso di richiesta e le PA del Gruppo A dovranno consolidare i loro servizi applicativi attraverso la gara SPC-Cloud. In realtà questa tempistica risulta già largamente disattesa. Il censimento delle infrastrutture ICT prevedeva come primo scaglione le Regioni, le Città Metropolitane e le società in house ICT, per poi proseguire con le Pubbliche Amministrazioni Centrali, le aziende sanitarie, le Unioni e i Comuni e poi a seguire tutte le altre PA. Il 23 aprile AgiD ha avviato questa seconda fase del censimento riguarda tutte le amministrazioni non comprese nella prima e che si dovrà concludere entro il 6 giugno. Al momento della chiusura di questo articolo sull'apposito sito web[8] non sono stati pubblicati dati relativi al censimento.–Diverse regioni si sono candidate e si stanno attrezzate per attivare Poli Strategici Nazionali (Marche, Puglia, Toscana, Sardegna), il Consorzio dei Comuni Trentini, il Progetto Tripolo delle Regioni Emilia Romagna, Friuli Venezia Giulia e della Provincia Autonoma di Trento.

Le recentissime circolari 2 e 3 2018 dell'AgID, pubblicate il 9 aprile 2018, contengono i requisiti e i criteri per la qualificazione rispettivamente dei Cloud Service Provider per la PA e di servizi SaaS per il Cloud della PA e consentono di delineare in modo più chiaro il quadro di riferimento dal punto di vista tecnologico per quanto riguarda le modalità di acquisizione dei servizi.

Quale è l'impatto sulle PA sia per quanto riguarda le infrastrutture hardware che i servizi software, in particolare quelli erogati in modalità SaaS? Per esempio nel caso di un sistema bibliotecario che già si avvale già di soluzioni applicative in cloud (anche nella forma più tradizionale hosting) quali scenari si prefigurano?

Per quanto riguarda l'infrastruttura, ovvero i data center, la circolare 2/2018 AgID definisce il processo, i requisiti tecnico-organizzativi ed i criteri di valutazione per qualificare Cloud Service Provider (CSP), che potranno fornire, gestire e amministrare i servizi Cloud di tipo infrastrutturale (IaaS, ovvero elaborazione, storage, connettività, sicurezza) e quelli di tipo piattaforma (PaaS, relativi agli ambienti di sviluppo applicativo e ai database). Si viene così a consolidare lo scenario infrastrutturale introdotto dal modello strategico e chiamato *Cloud PA* in cui le PA devono scegliere tra le seguenti tre alternative:

a) divenire o essere parte di un Polo Strategico Nazionale (PSN) certificato da AgiD
b) migrare il proprio data center verso i servizi Cloud-SPC del Contratto Quadro stipulato da CONSIP con il RTI aggiudicatario della Gara SPC-Cloud Lotto 1
c) migrare a un Cloud Service Provider (CSP) qualificato da AgID secondo il suddetto processo.

[8] https://censimentoict.italia.it/it/latest/

Per quanto riguarda i servizi applicativi di tipo SaaS le "Disposizioni per il procurement servizi SaaS per il Cloud della PA" emanate da Consip nell'ottobre 2017[9] hanno previsto un regime transitorio nel quale è proseguita la disponibilità delle offerte presenti nel sito Aquistinretepa (Me.Pa, Sistema Dinamico Acquisizioni e Convenzioni), mantenendo «comunque in capo alle singole Amministrazioni la responsabilità del rispetto della normativa nella fase di selezione e acquisto dei prodotti di tipo SaaS, attraverso gli strumenti di acquisto Consip ritenuti più idonei». Tale regime è cessato con l'emanazione della circolare AgiD 3/2018 (9 aprile) che fissa il processo, i requisiti tecnico-organizzativi ed i criteri di valutazione per la qualificazione dei servizi applicativi (SaaS) erogabili sul Cloud della PA. Lo scopo di questo processo di qualificazione è di consentire alle PA di utilizzare «servizi SaaS conformi ad un insieme di requisiti comuni» che assicurino l'aderenza a determinati modelli architetturali, il rispetto di alcuni principi organizzativi da parte dei fornitori, il livello di sicurezza, la performance, la scalabilità, l'interoperabilità e la portabilità e la conformità alle norme. Grazie a questo processo di qualificazione si verrà a creare il *Marketplace SaaS* e Consip provvederà ad aggiungere una nuova categoria di servizi che si affiancheranno a quelle già esistenti. Le Disposizioni Consip delineano anche la «eventualità» che i servizi SaaS già offerti nell'ambito del SPC-Cloud Lotto 1 debbano essere soggetti a qualificazione per poter essere inseriti nel *Marketplace SaaS*.

Pertanto tutti i sistemi bibliotecari che attualmente utilizzano soluzioni applicative SaaS (presumibilmente anche nella forma più tradizionale dei servizi in hosting) nell'affidare i loro servizi dovranno prestare particolare attenzione a valutare la conformità con le prescrizioni tecnico-organizzative del Piano triennale, i processi di qualificazione CSP e SaaS e le prescrizioni Consip relative all'acquisto di tali servizi.

Trattamento dei dati personali: il principio di responsabilità

Nel corso degli ultimi mesi, con l'approssimarsi del 25 maggio, data a decorrere dalla quale sarà pienamente operativo il Regolamento europeo GDPR, il trattamento dei dati personali è diventato di attualità e numerose sono le offerte di consulenza, formazione e strumenti sw di supporto che molte aziende stanno proponendo sia alle PA che alle imprese. Il recente episodio dei dati "sottratti" a Facebook dalla società Cambridge Analitica e usati per influenzare alcune campagne elettorali ha acceso i riflettori su una tematica troppo spesso sottovalutata sia perché ritenuta di pertinenza solo degli esperti di ICT sia per la scarsa sensibilità e cultura nel nostro paese riguardo alla tutela dei diritti dei soggetti interessati al trattamento dei propri dati. Il Regolamento prevede che i titolari dei trattamenti attivino una serie di azioni tra cui le principali sono:

a) la predisposizione del registro delle attività di trattamento dei dati personali
b) la valutazione dell'impatto sulla privacy prima dell'avvio di un nuovo trattamento
c) la nomina del Data Protection Officer
d) la previsione di meccanismi di protezione dei dati fin dalla progettazione delle attività e per l'intera gestione del ciclo di vita dei dati (*privacy by design e privacy by default*)
e) l'obbligo di segnalare al Garante e, in alcuni casi, anche agli interessati, la violazione sui dati (*personal data breaches*).

9 http://www.consip.it/sites/consip.it/files/Disposizioni%20per%20il%20procurement%20servizi%20SaaS%20per%20il%20Cloud%20della%20PA.PDF

In base la regolamento il titolare «determina le finalità e i mezzi del trattamento di dati personali» che comunque devono essere raccolti per finalità determinate, esplicite e legittime, trattati in modo lecito, corretto e trasparente, limitati e pertinenti a quanto necessario rispetto alle finalità del trattamento, aggiornati e conservati in forme che consentono l'identificazione degli interessati per un tempo non superiore a quello strettamente necessario al conseguimento delle finalità per le quali sono trattati, trascorso il quale devono essere cancellati o trasformati in una forma che non consenta di risalire all'interessato (pseudonimizzazione).

Ma l'aspetto più rilevante del regolamento è che tutte le prescrizioni e indicazioni sono fondate sul principio di "responsabilizzazione" (*accountability*) che consiste nell'obbligo per il titolare del trattamento di adottare le «misure adeguate ed efficaci», sia tecniche che organizzative, per garantire un'adeguata sicurezza dei dati personali trattati. Il titolare deve essere in grado di dimostrare la conformità delle attività di trattamento con il regolamento: è «opportuno verificare se siano state messe in atto tutte le misure tecnologiche e organizzative adeguate di protezione per stabilire immediatamente se c'è stata violazione dei dati personali e informare tempestivamente l'autorità di controllo e l'interessato» (considerando 87). Su richiesta il titolare dovrà dimostrare di aver adottato tutte le misure di natura organizzativa e tecnica appropriate a tutela dei diritti e della libertà degli interessati.

E' pertanto richiesto un cambiamento di mentalità poiché applicare ed essere conformi al regolamento non significa limitarsi implementare alcune misure e adempiere a determinate prescrizioni, ma attivare un processo di continuo monitoraggio e adeguamento dei trattamenti e delle misure che li accompagnano al fine di tutelare «i diritti e le libertà» delle persone fisiche interessate.

Riguardo allo scenario dei servizi in cloud discusso nei paragrafi precedenti un aspetto significativo è che il principio di responsabilità del titolare non viene meno nel caso in cui «altri abbiano effettuato per suo conto il trattamento dei dati» (Considerando 74). Proprio per tenere conto dei nuovi scenari di gestione ed erogazione dei servizi il regolamento definisce (Art.28) il «responsabile del trattamento» come «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento». Questa figura non deve essere confusa con quella di «responsabile della protezione dei dati» (DPO) che, nominato dal titolare, è un soggetto che opera in modo indipendente con funzioni (Art. 39) di consulenza, informazione e supporto (fornisce un parere in merito alla valutazione d'impatto) verso il titolare e che è chiamato a "sorvegliare l'osservanza" del regolamento riguardo all'intero processo di trattamento dei dati personali e a svolgere la funzione di collegamento con l'autorità di controllo.

Il processo di trasformazione previsto dal Piano triennale non solleva i titolari delle PA dalle loro responsabilità relativamente all'adeguatezza e all'efficacia delle misure da adottare per il trattamento dei dati personali, ma orientando verso l'uso di servizi in cloud implica la formalizzazione nei contratti di tutte le prescrizioni e garanzie atte a garantire che i soggetti responsabili dell'erogazioni di tali servizi (ai sensi del citato Art.28) adottino le misure e i comportamenti previsti dal Regolamento in base al quale titolari e responsabili potranno essere chiamati a rispondere delle eventuali violazioni e di comportamenti ritenuti non conformi dall'autorità di controllo che può applicare le sanzioni amministrative e pecuniarie previste dall'Art.83 (in base al tipo di violazione

accertata fino a 10M€ e per le imprese fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente).

I sistemi bibliotecari trattano dati personali e negli ultimi anni nei portali dei servizi e nei cataloghi online sono state introdotte funzionalità di tipo social che includono la possibilità di inserire recensioni, creare liste di testi preferiti, suggerire letture. I dati concernenti i prestiti, le ricerche sui cataloghi, gli scaffali privati e le interazioni di tipo social, sebbene gestiti allo scopo di orientare e razionalizzare le politiche di acquisto e di favorire la condivisione di interessi culturali e tematici tra gli utenti delle biblioteche, consentono anche di tracciare le azioni di questi utenti e costruire profili sui loro orientamenti, preferenze e relazioni che se usati in modo improprio o non adeguatamente protetti potrebbero esporre i soggetti interessati a illecite violazioni dei propri diritti e della propria libertà di opinione, credo religioso, orientamento politico e sessuale. Pertanto le biblioteche con l'entrata in vigore del GDPR, quali titolari dei trattamenti dei dati personali dei loro utenti sono chiamate a valutare attentamente le misure applicate per garantire la conformità alle disposizioni previste dal regolamento e il rispetto dei diritti dei propri utenti.

La sicurezza è una priorità

La transizione al digitale comporta naturalmente l'intensificazione di tutte le attività e le iniziative riguardanti la sicurezza del traffico di rete e dei sistemi, in primo luogo ove è previsto il trattamento di dati personali. Pertanto si rende necessario predisporre e avviare piani concreti investendo risorse, definendo priorità e dedicando la massima attenzione a questa tematica. A tal fine è indispensabile una continua e costante azione di informazione e formazione per rendere attenti sia gli operatori, nell'ambito esaminato i bibliotecari, che gli utenti alle possibili minacce e per sviluppare un insieme di competenze alla base delle quali deve esserci innanzitutto la capacità di utilizzare i servizi e le potenzialità della tecnologia in modo consapevole e responsabili.

La Direttiva europea 2016/1148 richiamata in precedenza e già in vigore prescrive che «gli Stati membri adottano e pubblicano, entro il 9 maggio 2018, le disposizioni legislative, regolamentari e amministrative necessarie per conformarsi».

Anche su questo fronte occorre registrare un forte ritardo in Italia poiché lo schema di Decreto legislativo per il recepimento della Direttiva è stato trasmesso al Senato il 21 febbraio 2018 ed è in attesa del completamento del suo iter.

Al momento sul piano concreto in tema di sicurezza è indispensabile far riferimento a:

- il Piano nazionale per la protezione cibernetica e la sicurezza informatica pubblicato nel
- Marzo del 2017dalla Presidenza del Consiglio dei Ministri[10]
- la Circolari AgID n. 1 e 2/2017, recante "Misure minime di sicurezza ICT per le pubbliche amministrazioni"[11] pubblicate in GU il 5 maggio 2017.

[10] https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/05/piano-nazionale-cyber-2017.pdf
[11] http://www.gazzettaufficiale.it/eli/id/2017/05/05/17A03060/sg

Quest'ultima circolare ha costituto al tempo stesso una prescrizione ed uno strumento di lavoro, infatti il responsabile di ogni PA per l'organizzazione, l'innovazione e le tecnologie (Art.17 del CAD) ha dovuto compilare e firmare digitalmente il "Modulo di implementazione" allegato alla Circolare. Tale modulo dovrà essere fornito al CERT-PA[12] italiano insieme alla notifica di eventuali incidenti e violazioni di sicurezza di cui siano stati oggetto i propri sistemi e servizi. Le "Misure minime" e il modulo hanno costretto ogni PA a confrontarsi con una griglia dettagliata di misure organizzative, comportamentali e tecnologiche attivando, almeno così è da augurarsi, quell'auspicabile processo di adeguamento senza il quale altrimenti non è possibile fronteggiare in modo proattivo ed efficace il crescente rischio di violazione dei dati e dei sistemi informatici e telematici.

Di fronte al mutato scenario dei servizi infrastrutturali e applicativi riassunto nei paragrafi precedenti se da un lato l'adozione delle infrastrutture Cloud PA rappresenta una semplificazione ed una razionalizzazione delle attività e degli impegni concernenti l'adozione delle misure di sicurezza, affidate ai gestori, dall'altro non viene meno la responsabilità in termini di prerequisiti contrattuali, monitoraggio e accertamento che le misure siano adottate e implementate correttamente. Inoltre il sottoinsieme di misure previste per costituire l'inventario dei sw autorizzati e non autorizzati, per proteggere le configurazioni hw e sw sui dispositivi mobili, i laptop e le stazioni di lavoro, per attivare le difese contro i malware richiedo una piena attuazione sia per quanto riguarda le postazioni di lavoro del personale delle biblioteche sia di quelle a disposizione degli utenti delle biblioteche per i quali occorre prestare un'attenzione particolare all'utilizzo dei dispositivi personali.

Conclusioni

Non vi è dubbio che le biblioteche pubbliche sono chiamate come ogni PA a confrontarsi con un uno scenario estremamente complesso e articolato che sta accompagnando la trasformazione al digitale della PA italiana. Le lentezze, i ritardi e le lacune evidenti sia per quanto riguarda le norme che i piani rappresentano un fattore di criticità che aumenta la complessità di questa fase di transizione. Tuttavia le biblioteche ed i bibliotecari sono avvantaggiati rispetto ad altri settori della PA avendo già da molto tempo intrapreso il percorso della trasformazione e avendo maturato attraverso progetti e realizzazioni innovative competenze e consapevolezze che potrebbero risultare di estrema utilità se riconosciute, valorizzate e condivise con gli altri ambiti della PA attivando sinergie e collaborazioni.

[12] https://www.cert-pa.it/